[H.A.S.C. No. 114–112]

HEARING

ON

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2017

AND

OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES HEARING

ON

FISCAL YEAR 2017 BUDGET REQUEST FOR U.S. CYBER COMMAND: PREPARING FOR OPERATIONS IN THE CYBER DOMAIN

HEARING HELD
MARCH 16, 2016

U.S. GOVERNMENT PUBLISHING OFFICE

20–064 WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

JOE WILSON, South Carolina, *Chairman*

JOHN KLINE, Minnesota
BILL SHUSTER, Pennsylvania
DUNCAN HUNTER, California
RICHARD B. NUGENT, Florida
RYAN K. ZINKE, Montana
TRENT FRANKS, Arizona, *Vice Chair*
DOUG LAMBORN, Colorado
MO BROOKS, Alabama
BRADLEY BYRNE, Alabama
ELISE M. STEFANIK, New York

JAMES R. LANGEVIN, Rhode Island
JIM COOPER, Tennessee
JOHN GARAMENDI, California
JOAQUIN CASTRO, Texas
MARC A. VEASEY, Texas
DONALD NORCROSS, New Jersey
BRAD ASHFORD, Nebraska
PETE AGUILAR, California

KEVIN GATES, *Professional Staff Member*
LINDSAY KAVANAUGH, *Professional Staff Member*
NEVE SCHADLER, *Clerk*

CONTENTS

FISCAL YEAR 2017 BUDGET REQUEST FOR U.S. CYBER COMMAND: PREPARING FOR OPERATIONS IN THE CYBER DOMAIN

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES,
Washington, DC, Wednesday, March 16, 2016.

The subcommittee met, pursuant to call, at 2:03 p.m., in room 2212, Rayburn House Office Building, Hon. Joe Wilson (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. JOE WILSON, A REPRESENTATIVE FROM SOUTH CAROLINA, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. WILSON. Ladies and gentlemen, I call this hearing of the Emerging Threats and Capabilities Subcommittee of the House Armed Services Committee to order.

I am pleased to welcome everyone here today for the hearing on the fiscal year 2017 budget request of the United States Cyber Command. Since we last met to talk about the work of USCYBERCOM, the news has been filled with stories that remind us of the critical job facing the Department of Defense [DOD], from the intrusion on the Joint Staff networks to the compromise of personal information of millions of government personnel and their families.

Cyber is proving to be both a domain of warfare on its own as well as a key enabler for all other domains of war. In looking through this most recent budget request, we should be asking ourselves some important questions.

Do we have the resources, people, cyber tools and training needed to be effective?

Do we have the necessary policies and authorities to conduct cyber operations?

What areas require additional refinement?

Are we deterring potential adversaries and contributing to our overall national security?

As we tackle these tough questions, I would like to take the opportunity to welcome back as our witness today, Admiral Michael Rogers, commander of U.S. Cyber Command.

One of the major tests that our Admiral Rogers has to contend with is how to operate in an environment in our interagency, international, and industry partners. I am pleased to hear that in a major upcoming exercise entitled Cyber Guard 2016, personnel from the House administration staff will be participating. I am especially looking forward to hearing the plans for that exercise and

how we might also apply its lessons in defending the House of Representatives' networks.

I would like now to turn to my friend, Ranking Member Congressman Jim Langevin from Rhode Island, for any comments he would like to make.

[The prepared statement of Mr. Wilson can be found in the Appendix on page 27.]

STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. Well, thank you, Mr. Chairman. I want to welcome Admiral Rogers back before the subcommittee today. It is an honor to have you here, Admiral, and appreciate all you are doing to protect our Nation's cyberspace and certainly look forward to discussing cybersecurity and operational fiscal year 2017 budget request for U.S. Cyber Command across the Department.

I have been one of the biggest proponents of cybersecurity as a critical warfighting domain during my time in Congress. So I am pleased to discuss this vital piece of our national security here with you today.

As we know, cybersecurity and cyber operations are paramount in today's world, from defending the DODIN [Department of Defense Information Network], to deterring and defending against adversaries, to meeting combatant command needs. Cyber is a key component of all strategies across every aspect of national defense and security.

As such, the total cybersecurity and cyberspace operations budget for the DOD is $6.8 billion for fiscal year 2017 and ranges from protecting data to operating in the domain.

Now, of that investment approximately $505 million is requested for Cyber Command. Now, the funds requested for the service cyber components to mature the command and increase the capacity of cyber mission forces [CMF] make up a substantial portion of that request.

While we have made tremendous progress in this area, significant investment over the Future Years Defense Program will still be required. And as the CMF matures we must work to synchronize investments made by services in other agencies.

Now today, I look forward to receiving an update on the CMF, particularly with regard to the readiness of our service cyber components to meet the initial and fully operational capability goal dates for the teams, as well as the challenges and risks associated with meeting those mandatory deadlines.

We must have the right number of teams, but just as importantly we must also have a ready force that is manned, trained, and equipped to meet the mission.

I am particularly pleased that Cyber Command has made progress in measuring readiness. Now, since last year strides have also been made in establishing a persistent training environment, a necessity for preparedness.

Today I hope to hear more about the steps Cyber Command has taken since last year to promote a joint environment with common standards such as issuing guiding frameworks for doctrine, organi-

zation, training, leadership, education, and policy, as well as whether or not capability baselines for cyber protection teams have been established to ensure interoperability and aligned investments.

With respect to the cyber teams' missions, there is a whole host of policy questions we must address as we continue to mature our offensive and defensive capabilities and operations.

I believe it is imperative that we understand lessons learned from real world experiences about command and control of teams and their various roles in missions, capabilities required, authorities used, and new authorities that may be required for more effective operations as well as internal-external oversight.

So finally, Mr. Chairman and Admiral, I look forward to hearing about the status of the implementation, acquisition, and personnel management authorities that were granted in the fiscal year 2016 NDAA [National Defense Authorization Act].

So I know it is a lot to cover, Admiral. You have got a lot on your plate. I appreciate the extraordinary work that you and your team do at Cyber Command or at NSA [National Security Agency] are doing to protect our country in cyberspace and leverage all the capabilities for the benefit ultimately of our warfighter and our national defense.

So with that, thank you again for testifying here today, Admiral Rogers, and thank you for your service to our Nation.

And Mr. Chairman, thank you for your attention, your focus and your support on this issue especially. And I yield back.

Mr. WILSON. Thank you, Congressman Langevin.

I am grateful, Admiral Rogers, that your written statement has been submitted for the record. So we ask that you summarize your comments within the 5-minute rule, which is applicable to all of us and being well-maintained by Kevin Gates.

Admiral Rogers, please begin.

STATEMENT OF ADM MICHAEL S. ROGERS, USN, COMMANDER, U.S. CYBER COMMAND

Admiral ROGERS. Before my clock starts, I would like to start with we should be doing this outside given how beautiful the day is. We should be outside.

With that, Chairman Wilson, Ranking Member Langevin, distinguished members of the committee, I am pleased to appear before you today to discuss the opportunities and challenges facing Cyber Command. And I would like to thank you for convening this forum.

It is an honor to represent the individuals of this fine organization, and I am grateful for and humbled by the opportunity to lead this impressive team. I am confident you would be extremely proud of the men and women of Cyber Command if you saw their commitment to mission and hard-earned success on a daily basis as I do.

While my written statement goes into greater detail, I would like to briefly highlight the challenges we face in today's environment and also some of the initiatives the command is pursuing to meet these challenges.

Since I testified last year, U.S. Cyber Command has seen an intensification of cyberspace operations by a range of state and non-

state actors. We have seen a wide range of malicious cyber activities aimed against both government and private sector targets.

At U.S. Cyber Command we focus on foreign actors that pose a threat to our national interests through cyberspace. At this time nations still present the greatest or gravest threats to our Nation's cybersecurity because they alone can commit the significant resources needed to sustain sophisticated campaigns to penetrate in our best-guarded networks.

But we continue to also look closely for signs of non-state actors making significant improvements in their cyber capabilities. The states we watch most closely remain Russia, China, Iran, and North Korea. The self-proclaimed Islamic State is also a concern, although mainly for their use of cyberspace propaganda and recruiting.

In general, these actors conduct a range of cyber activities to support their state's interest. They steal intellectual property, citizens' personal information, and they have intruded into networks ranging from the Joint Staff's unclassified network to networks controlling our Nation's critical infrastructure.

These threat actors are using cyberspace to shape potential future operations with a view to limiting our options in the event of a crisis.

Despite this challenging environment, Cyber Command continues to make progress as its emphasis shifts to operationalizing the command and sustaining its capabilities.

Over the past year we have continued building the capability and capacity of Cyber Command while operating at an ever-increased tempo. We continue to make progress in building a cyber mission force of the 133 teams that will be built and fully operational by 30 September 2018. Today we have 27 teams that are fully operational and 68 that have attained the initial operating capability landmark.

And it is also important to note that even as teams that are not yet fully operational or have even met our initial operational capability, they are contributing to our cyberspace efforts with nearly 100 teams or elements of those teams conducting cyber operation to include teams that are supporting Central Command's ongoing efforts to degrade, dismantle, and ultimately defeat ISIL [Islamic State of Iraq and the Levant].

Last year I noted we had just established the Joint Force Headquarters [JFHQ] DOD Information Networks, or DODIN. Today I can proudly report that JFHQ–DODIN has made great strides towards its goal of leading the day-to-day security and defense of the Department's data and networks.

Also as the DOD expands the Joint Information Environment we will have significantly more confidence in the overall security and resiliency of our systems. Our operations to defend DOD networks and the Nation's critical infrastructure proceed in conjunction with a host of Federal, industry, and international partners.

No single agency or department has the authority, information, or wisdom to accomplish this mission alone, which is why Cyber Command recently updated our understanding with both NSA and the Department of Homeland Security in a cyber action plan to chart our collaboration.

Our cyber mission forces continue to operate safely and in a manner that respects the civil liberties and privacies of American citizens. Additionally, cyber mission teams and joint cyber headquarters are regular participants in the annual exercises of the combatant commands.

Cyber Command's only annual exercises, as you have highlighted, Cyber Flag and Cyber Guard offer unmatched realism as we train with Federal, State, industry, and international partners. And while our training is improving we need a persistent training environment which the Department is continuing to develop to gain necessary operational skills and to sustain readiness across the force.

Cyber Command is also actively contributing to the implementation of the new DOD cyber strategy. Senior leaders at the command are leading or serving on teams charged with implementing the strategies and the initiatives, particularly the lines of effort regarding the training and proficiency of the cyber mission force and the broader cyber workforce across the Department, as well as the integration of cyber effects and DOD and cross-agency planning efforts.

To help with all of this we needed enhanced acquisition and manpower authorities, and I thank Congress and the President for the authorities granted to Cyber Command in the fiscal year 2016 National Defense Authorization Act. This represents a significant augmentation of our ability to provide capabilities to our cyber mission teams, as well as our ability to attract and retain a skilled cyber workforce.

We are now studying how to best implement the Act's provisions and laying the groundwork needed to put them into effect while in parallel evolving a formalized synchronization framework to operationalize and optimize the employment of cyber mission forces.

Let me assure the committee that despite the challenging cyber environment we operate in, Cyber Command continues to make significant progress, all while simultaneously conducting cyber operations against determined adversaries.

Additionally, the command has a clear path ahead and is actively pursuing new initiatives and authorities to best position the command to address the challenges and opportunities that we will undoubtedly confront.

With that, thank you again, Mr. Chairman and members of the committee for convening this forum and inviting me to speak. And I look forward to your questions.

[The prepared statement of Admiral Rogers can be found in the Appendix on page 28.]

Mr. WILSON. Thank you very much. And we now will proceed, and Mr. Gates will maintain the 5-minute rule on behalf of all of us as we rotate.

And Admiral, I want to thank you again. It is a challenging environment. There are gruesomely capable adversaries, but I just appreciate your service and your colleagues and however we can back you up.

And in regard to that, currently, is the throughput of the training pipeline a limiting factor in our ability to get cyber mission

teams up and running? And if so, do you have any suggestions on how to improve that situation?

Admiral ROGERS. So it is probably the single greatest limiting factor at the moment. It is a little uneven. It impacts more services than others. I would argue at the moment it is probably having more impact on the Air Force probably than any other services.

In fact, I just met with all of my service component commanders in February. We reviewed where we are in bringing the mission force online. That review highlighted that to meet initial operational capability for the force we will have 91 percent of that completed on time. That means 9 percent behind, so I have got between now and the end of the year to figure out what are we going to do to get that 9 percent back online.

I have already seen some improvement just in the 6 weeks, and I, in fact, have highlighted the results of that review with the service chiefs as well as the chairman and the vice chairman. So we are working collectively as a Department to move forward.

That review also highlighted that when it comes to full operating capability, which is the final milestone, if you will, that is all 133 teams and at full capability by 30 September of 2018, that right now we assess as of February in the last review 93 percent of the force will be delivered on time. And we have 7 percent that we have got to get back online. I have got 2 years to do that.

I am confident that we are going to be able to do it. And as you have said, I would highlight right now training throughput probably the single greatest limiting factor.

Mr. WILSON. And is there anything that we can do to help?

Admiral ROGERS. At the moment I am still working with the Air Force in particular. I am not ready to come to you and say I need more external help. I want to make sure we have exhausted everything that we can do internally.

Mr. WILSON. Well, if there has ever been strong bipartisan support——

Admiral ROGERS. Yes, sir.

Mr. WILSON [continuing]. It is people who are here today who want to back you up.

Additionally, could you explain the capabilities development group and give us highlights of their work?

Admiral ROGERS. So it is a capability that we carved out at Cyber Command because one of my observations was, and I have said this to the committee before, I believe fiscal year 2016 is a tipping point for us as an organization where we will go from a focus on developing capacity to a focus on actually employing the capacity that we have been developing over the last 3 years. You see that reflected in the range of both defensive and offensive real world operations that we are doing right now.

And so part of our capability to do that is generating very specific technical and operational capabilities. And so I felt we needed to carve out a segment of the team that was partnering with the private sector, the rest of DOD, other elements of the government, as well as NSA about how can we bring together those capacities to generate actual outcomes in capacities and capabilities that we can employ with the force.

Mr. WILSON. Well, so——

Admiral ROGERS. So we stood that up.

Mr. WILSON. Well, again, thank you for being innovative. How are you addressing new and emerging cybersecurity challenges not directly related to the network like vulnerabilities to datalinks, weapons systems, industrial control systems, or the Internet of Things?

Admiral ROGERS. Right. So just a few challenges there with that statement.

[Laughter.]

Mr. WILSON. And I am glad Congresswoman Stefanik is here because she understood what I asked.

[Laughter.]

Admiral ROGERS. So what I have tried to do is prioritize. I have said industrial control systems and SCADA [Supervisory Control and Data Acquisition] probably is the next big area for us because we have got to transition from a focus purely on the network structure. We have to retain that but we have got to move into other areas.

The other areas that really concern me when I look at the problem set are platforms and systems and getting down to individual data concentrations across the Department. We have started an effort to look at data concentrations, a focus industrial control systems and SCADA.

I would highlight in this regard some great work, for example, that the Guard and Reserve are doing. I highlight specifically out in Washington State the Army National Guard is really doing some interesting work that we are partnering with them on. In fact, the Secretary was just out there to take a look at that about 2 weeks ago.

The challenge for now, because I want to set everyone's expectations in a realistic way, I mean, what I have told the leadership of the Department is I acknowledge that this is what we have to do, but we have finite capacity.

So it is all about I have to prioritize and then we have got to figure out who are the other partners that we have who could bring additional capacity to help us in this fight. And we are in the process of doing that.

Mr. WILSON. And for the benefit of me, can you identify what the Internet of Things means?

Admiral ROGERS. So increasingly what you are finding is in the production of almost—increasingly everything we—refrigerators, automobiles, your iron. I was looking at an Internet-connected iron, for example, just a little while ago. Increasingly those everyday devices that we take for granted in the lives we lead are being connected with each other, designed to increase their capability.

For example, a refrigerator, would you be interested in a consumer if your refrigerator was able to tell you what your current milk load is in the refrigerator and when are you going to need to buy more? Could it do that automatically?

Could you do upgrades, for example, to systems that you are buying now automatically remotely so that you don't have to physically take that device into a dealer or the manufacturer, they can do it remotely. So increasingly you are finding this connectivity prolifer-

ating across almost everything that we are building and buying these days.

Mr. WILSON. Well, thank you so much.

And we now proceed to Congressman Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Yes, it is a bolder world out there, Admiral, for sure. It is just scary, challenging, and fascinating all at once.

Well, with respect to cyber mission force issues, policy, authority, and doctrine are paramount to effectively employing the cyber mission force. Yet those key ingredients lag behind our talent pool and toolsets.

Now, given that the cyber domain is a relatively new operating environment and the strategic implications associated with operating in that environment, I understand why policy, doctrine, and authorities have taken time to develop.

Now that said, state and non-state actors continue to be aggressive in this environment, and we must move forward. So this committee must also understand how they are developing and being formalized so that we can assist where needed and obviously conduct oversight of activities.

So my question is how are real world events such as the OPM [Office of Personnel Management] and Joint Staff incidents and counter-ISIL operations influencing and shaping policy, authorities, and doctrine are required to effectively employ our force?

Admiral ROGERS. So if you take a look at Cyber Command's three mission sets—it is kind of the way I have been doing it—so what are the acquisitions and the authorities that we require to make sure we are able to execute each of those three missions in an effective and efficient manner?

So the first mission, defense of the DOD networks, I am very comfortable that we have all the authorities that we need and that I can do what I need to do in a timely manner within the Department to defend our networks.

The second mission is about our ability to generate capacity and capability to support the combatant commanders from the defensive to the offensive. That is an area where quite frankly we are trying to use our work, which again, I am not going to discuss in any great detail in an unclassified setting, but we are trying to use some of the real world insights that you highlighted several of them, ISIL, the last major intrusion we dealt with, which is now almost a year ago.

We are asking for the authorities we need for that and I would highlight, boy, we are seeing a massive amount of change within the last 6 months, so I am very comfortable that we have identified the requirements.

We have got endorsement for what we need to do and in fact I am expecting the last couple of changes we will ask for will be signed out by the end of the month.

The one area that I think is still where we still need more collective work, and I need to work on this, too. I don't want to make it sound as if I am trying to put anyone else on report. Is how do you apply DOD-generated capacity in the cyber arena outside the government in the private sector?

That is probably the area where I would say we still need to do more work. I will be honest. It hasn't been my highest priority. As I have told you every time generally when we meet I always remind everybody, look, there is such a disconnect between the requirements of this mission set and where we are in capability. It is all about prioritization and making smart investments.

And so I have consciously prioritized along those three missions that I just discussed. So it is the next big area that we really have got to get into.

Mr. LANGEVIN. Thank you, Admiral. What does Defense Support of Civilian Authorities look like for cyber? And in our current framework—is our current framework applicable to the cyber domain?

Admiral ROGERS. So that is a part of our previous discussion about this fact. I think it is the area where we still need the most work, as I know you are aware. We have an existing framework, DSCA, Defense Support to Civil Authorities, that we currently have in place that talks about how the Department will employ its capabilities in support of civil authorities.

That structure has been used for decades from tornado and, you know, and hurricane, natural disaster response to a host of other capabilities. It does not as currently written explicitly address cyber.

So it is one of the areas that we are collectively stepping back and asking ourselves, so how does the DSCA construct apply to cyber and what is the most effective and efficient way to use it? Because my attitude is, and it is not unique to DSCA, let us start where cyber is very similar to the other mechanisms we have already put in place. Don't reinvent the wheel every time just because it is cyber.

And so we have a framework right now through DSCA for how the Department provides capacity and capability to support external civil authority. I think it is an area, as again I have said previously though, we have to dig into a little bit deeper about how are we going to do that in the cyber arena?

Mr. LANGEVIN. Okay. Maybe to further drill down on this, what are best practices from capability development to leadership development are you seeing from the services? And what steps are you taking to institutionalize these best practices across the services?

Admiral ROGERS. So I am going to combine that question with a previous where you asked about, for example, what have you learned from previous events like OPM and the Joint Staff intrusion? One, and I will just use this as one example, one of our takeaways for our effort on the Joint Staff was we needed to do a better job of formalizing a common set of tools, defensive tool capabilities across all the defensive teams that we were creating.

And so I went to each of the services and said, so let us talk about what is the best of breed, what are the best of capabilities that we have identified within each service that we can port across the entire enterprise? Let us not spend a lot of time and money with everybody independently trying to develop similar capabilities.

So in fact the Air Force has a tool that we were very impressed with, and I am currently working with the services to let us adopt this. This is the standard across the Department. We don't need to

do four different funding streams here to go after the same problems sets.

We do that with respect to we regularly review training standards and training equivalencies and when Army, for example, has developed some capabilities in terms of the development of training standards where they have come back to us and asked that we adopt this, which we have agreed. I have talked about, hey, let us use this across the entire Department.

So we try to do it in a very systematic ongoing way because I am a big fan of we have got to be more efficient and, you know, we have got to be faster. And the best way to do that is to look across an entire enterprise, both within the Department as well as what we are trying to do outside the Department.

I won't get into that right now for this question, but I am sure you will ask me about that later what we are doing outside the Department to try to do those same kinds of things.

Mr. LANGEVIN. Very good. Thank you, Admiral.

I yield back, Mr. Chairman.

Mr. WILSON. And thank you, Mr. Langevin.

We now proceed to Congressman Mo Brooks, of Alabama.

Mr. BROOKS. Admiral Rogers, how much is the Cyber Command requesting for this year?

Admiral ROGERS. Slightly over $500 million.

Mr. BROOKS. How much funding did the Cyber Command receive for fiscal year 2016, the current year?

Admiral ROGERS. Slightly under $500 million. It was, if my memory is right, $488 million, and the 2017 budget request is an approximate 9 percent increase over our 2016 authorization.

Mr. BROOKS. What was it in fiscal year 2015?

Admiral ROGERS. I apologize, sir. I don't know it off the top of my head.

Mr. BROOKS. Do you recall by any chance for fiscal year 2014?

Admiral ROGERS. No. I don't. I apologize.

Mr. BROOKS. My recollection and the reason I was asking this is try to get better information than just my recollection, is that the Cyber Command has had significant increases over the last 3 or 4 years. Would that be a fair statement to the best as you can recall?

Admiral ROGERS. I would phrase it as our funding has increased in a systematic way over the last few years.

Mr. BROOKS. The reason I bring this up, and I am not sure if you are familiar with it, but America's financial condition has taken a fairly stark turn for the worse.

Just to iterate some of the numbers, the Congressional Budget Office [CBO] is warning us that in about 6 years we are going to hit a string of trillion dollar a year deficits until such time as whatever really bad can happen happens. In my judgment it would be a debilitating insolvency and bankruptcy of our country.

This year the CBO is telling us that our deficit is going to be $105 billion worse than last year at $544 billion. In terms of our budget, we are right now having some pretty intense discussions in Congress about our $1.07 trillion budget. Keep in mind that there is a lot more off-budget entitlement programs, debt service, and whatnot.

But if you have $1.07 trillion in budgetary items that you actually have control over and have to vote on each year, that means that right now we are being asked to borrow about half of what we spend, a little bit over 50 percent. Money we don't have; can't afford to pay back once we borrow it.

And all this is coming to a head. What efficiency measures can the Cyber Command implement in order to help the taxpayer get more bang for the buck for the day when we start seeing sizeable cuts across the board in defense and every place else simply because we have run out of money and we have run out of borrowing capacity?

Admiral ROGERS. So we have been doing that since the day U.S. Cyber Command was created. It is one of the reasons, for example, why the Department decided to align U.S. Cyber Command and NSA very closely. That the idea was don't replicate the billions of dollars of investment that the Nation has made in generating cyber expertise, for example, at the National Security Agency.

Rather than replicate that scale of investment in U.S. Cyber Command how can you align them so Cyber Command can take advantage of the investments that have already been made? It goes into the way Cyber Command prioritizes. As I constantly tell the team, nobody gets a blank check. Nobody gets a blank check.

Mr. BROOKS. Well, if we are improving efficiency normally that means that you are getting more done for the same or less or fewer dollars. Why then the request for an increase in spending——

Admiral ROGERS. Because I would argue, sir, look at the world around you.

Mr. BROOKS. I understand it is a very dangerous place.

Admiral ROGERS [continuing]. As well. We can't——

Mr. BROOKS. Okay. Let us assume for a moment then——

Admiral ROGERS. If I could just finish the thought? Sorry, sir.

Mr. BROOKS. Go ahead.

Admiral ROGERS. And I, please, don't mean to be rude or——

Mr. BROOKS. No, that is okay.

Admiral ROGERS. But just to finish the thought.

Mr. BROOKS. I get interrupted all the time.

[Laughter.]

And I apologize for when I interrupt you. Go ahead.

Admiral ROGERS. This is not a mission set that we are going to efficiency our way out of. I just don't believe that that is achievable. In no way should you take from that comment, so Admiral, are you telling me that you don't have a responsibility to the citizens of this nation to execute your mission in an efficient and effective way? That is not what I am saying.

But my only point is the investments that we are making in cyber reflect the nature of the world we are dealing with from a threat perspective. Even as we acknowledge that that threat picture is occurring in an environment in which resources are very tight. I am the first to acknowledge that.

So what I try to do as a commander, what I try to do as a citizen, is make sure that what Cyber Command is doing is prioritized, realizing we can't do it all. We try to space events out over a reasonable period of time. That is what I try to make sure we do because I think you raise a very valid concern. I am the first to——

Mr. BROOKS. Okay. I get the argument we have a growing threat matrix therefore we need more funding in order to properly defend against that greater threat.

Now, let us assume for the moment that there aren't any efficiencies that you can implement that would allow us to have the kind of security we want at current funding. Where do you suggest the money come from in the defense budget in order to help with Cyber Command?

Admiral ROGERS. Fortunately, sir, that is not the role that I play.

Mr. BROOKS. I thought I would ask anyway, but I understand.

Admiral ROGERS. [Laughter.]

Mr. BROOKS. Thank you, Mr. Chairman. I yield back.

Mr. WILSON. And thank you very much, Congressman Brooks.

And we now proceed to Congressman Brad Ashford, of Nebraska.

Mr. ASHFORD. Thank you, Admiral.

Admiral ROGERS. Sir.

Mr. ASHFORD. And since I have been here it is just amazing how quickly from when we had these discussions when I first met you 8, 14 months ago where we are today is——

Admiral ROGERS. Right.

Mr. ASHFORD [continuing]. Beyond remarkable. I have a lot of questions and I know—well, just training for the moment. Do you see the—and you already have these collaborations with academia and others to help train and increase training capabilities. Do you see an enlargement of that utilizing almost a UARC [University Affiliated Research Center] model? As for an example, I mean, I know where UARC in Nebraska, there is MIT's [Massachusetts Institute of Technology's] UARC.

Admiral ROGERS. Right.

Mr. ASHFORD. They have all these various ones. How do you see—if the mission is training more and more cyber people, is that an avenue to do that?

Admiral ROGERS. I mean——

Mr. ASHFORD. Or how do you see that happening?

Admiral ROGERS. I think that is clearly a role. One thing I try and remind people when it comes to training I think one of the important things is we must ensure that the output we generate is standardized across the entire force.

Mr. ASHFORD. Right.

Admiral ROGERS. Because if we don't do that, I believe we are going to run into challenges when it comes to actually employing that force. So one of the things that I have been very insistent on, even as we partner across the total force in DOD and we look at broader partnerships outside the DOD for the mission force that we are creating, is that the team standards, the training approaches we take, the certification standards that we put in place, we have got to standardize those.

Now, within those standards what I tell the team is, look, I am open to what are the options that are out there? And clearly academia and the private sector are part of that solution set.

To date we have tended to use them more on the capability side development, if you will, than we have on the training side, although we are doing some things on the training side. But to be honest, I would say to date it has been more on the capability side.

Mr. ASHFORD. What I see in my area, companies like, you know, First Data, Mutual of Omaha, whatever it is, everybody has those kind of corporate presence somewhere in or near their districts.

And then we have STRATCOM [U.S. Strategic Command]. So what we have, for example, in Omaha area is STRATCOM, and numbers of employees at STRATCOM that are contractors, were in the military, whatever, with IT [information technology] backgrounds going back and forth either working at STRATCOM or to Offutt or coming back into the private sector.

And there are just a huge number of these people in varying degrees of capabilities, some younger, some retired. Maybe you have answered this, but how do you organize that? I mean, there is a clear force there and a lot of capability. How do you bring them and exchange them back and forth? How would that work?

Admiral ROGERS. So in fact right now one of the things we have started in the last year since our last budget testimony to take the idea that you have articulated, which is how do you harness the capabilities resonant in the private sector, particularly those people——

Mr. ASHFORD. Right.

Admiral ROGERS [continuing]. Who either have previous DOD experience——

Mr. ASHFORD. Right.

Admiral ROGERS [continuing]. And who are now operating in the private sector? So we have created out in Silicon Valley what we call the United States Cyber Command Point of Partnership or Point of Presence.

We have tied it into the broader DIUx [Defense Innovation Unit Experimental] effort, and what we have done is I put one active individual out there, but then we have identified a team of prior military individuals currently working in Silicon Valley in different companies, and we are asking ourselves can we use this as an incubator for a model that we can employ elsewhere?

We have done it in Silicon Valley in the last year. I was just in Boston at the end of last week. We are going to use Boston as our second test case because of the IT capabilities there. And then I am looking to see does this scale into others, Omaha, for example.

Mr. ASHFORD. Yes.

Admiral ROGERS. There are about five that we have identified that are possibilities for the future.

Mr. ASHFORD. Yes, I mean, I think it is an incredible concept and to me it is amazing how quickly you have implemented this because just a year ago when you were talking about it——

Admiral ROGERS. Yes, sir.

Mr. ASHFORD [continuing]. This idea and there is just this abundance—and I will let it go, Mr. Chairman because I am being redundant a bit here. But is that it is amazing the appetite on the private sector that, you know, these major companies give us a way to help and then we have got all this capability or whatever. But you do have to have standards obviously.

Admiral ROGERS. Right.

Mr. ASHFORD. And then this whole group of retired or, you know, military personnel at STRATCOM, it is just to harness that. And you are capturing that. It is very exciting, and I appreciate your

efforts. I think the incubator idea is great, Center of Excellence, whatever you want to call it.

Thank you, Mr. Chairman.

Admiral ROGERS. If I could, just one quick comment? I was out in the valley 2 weeks ago talking to the team. It is one of the most energizing—I mean——

Mr. ASHFORD. Yes.

Admiral ROGERS [continuing]. Watching these men and women talking about how they can take advantage of what they are doing every day with company X, Y, or Z in the valley and how they want to harness their knowledge——

Mr. ASHFORD. Yes.

Admiral ROGERS [continuing]. And their military experience.

Mr. ASHFORD. And I see that. We meet with these companies all the time in Omaha. The first question they have is how can we help——

Admiral ROGERS. What can I do?

Mr. ASHFORD [continuing]. The military, too? Thank you, Mr. Chairman.

[Laughter.]

Mr. WILSON. And then thank you, Congressman Ashford, and it is encouraging to see Secretary Carter and the public-private cooperation.

And speaking of good cooperation, Congressman Doug Lamborn all the way from Colorado.

Mr. LAMBORN. Yes, thank you, Mr. Chairman. And you came all the way from South Carolina.

[Laughter.]

Mr. LAMBORN. Anyway, Admiral, I am going to build on some questions that have already been begun by my colleague, Representative Ashford, but he was talking about you were responding corporations in the private sector and academia.

What are ways of just fostering this private-public partnership? If there is anything more you could add to that? Because I know there are folks in Colorado Springs that are very keen on this as well.

Admiral ROGERS. Yes, sir. So a couple things come to mind. We have created an exercise series, you heard it in my remarks and the chair mentioned, that we call Cyber Guard where once a year we pick a problem set. We come up with an exercise scenario that crosses the Nation so we can bring together entities from across the Nation.

We bring together private companies, State, local, and Federal actors, Cyber Command and the Department of Defense as well as commercial infrastructure providers, for example, and we outline a problem set.

We actually create a notional network that reflects if we are modeling for example an attack against the power structure. We actually in partnership with some of the power companies we develop a network simulation that replicates the network associated with a large utility.

We have done this in multiple areas. This exercise scenario occurs every June. We ask private companies if you want to partici-

pate we would love to have you. We are up to about 100 right now. We just started this in the last 3 years.

And I can remember the first one we did we had about three. It is getting to the point now where I am starting to run into a capacity concern where we have got more interest than there is room.

In addition, I am also doing this more on the NSA side first, but the other area that I have tried to highlight potentially with the private sector is, is there a way to take some of our DOD workforce, have it spend some time in the private sector, and then come back to us? And is there a way also to have the private sector spend some time with us?

That hasn't been a traditional DOD model. And, boy, it certainly hasn't been the traditional Intelligence Community model in my other job. But my view is that that is kind of among the things that we have got to do for the future. We have got to view this as much more of a broader partnership.

One of my takeaways is, I mean, this is just the ultimate team activity. I have never done so much private sector and interagency work in 35 years of military service.

Mr. LAMBORN. Well, and academia as well.

Admiral ROGERS. Yes, sir, which is why I was just up at Harvard on Thursday when I was up there. I have been to Carnegie-Mellon, Berkeley, and Stanford in the last 8 weeks trying to talk to the private sector about, hey, what can we do? I am actually in Colorado Springs in 30 days. Going to spend some day out there working on a couple things.

Mr. LAMBORN. That is wonderful. And I like that idea of private-public partnership, collaboration, teamwork and maybe with some of our allies. What are your thoughts on working with allies, you know, Israel or some of the NATO [North Atlantic Treaty Organization] allies?

Admiral ROGERS. Right. So I won't get into the particulars, but in fact today U.S. Cyber Command is hosting a deterrence workshop with one of our allies that you just mentioned. I am not going to say which one.

In addition we are doing partnerships and capabilities development probably with, you know, five or so key nations right now, foreign nations. In addition, we are also doing things in a much broader front talking about cyber theory, cyber defense across the NATO alliance, and literally with nations around the world. It is one of the reasons why I spent some time on the road, you know, internationally.

Mr. LAMBORN. Lastly, with the limited time I have, let me shift gears. Everyone knows the Guard and Reserve make a wonderful component of this effort. You can do cyber from anywhere. And we find Guard and Reserve all throughout the country.

You can do it anytime. And of course their schedules are, you know, 24/7 as well. Given the wealth of knowledge, experience, and certifications in the Guard and Reserve would it be prudent to consider a streamlined accessions process to get these specialists onto the job quicker?

Admiral ROGERS. I don't intellectually disagree. The only comment I would make is in my discussions with the Guard and the Reserve segment when I have asked so do you have issues that I

can help with in terms of your ability to assess and bring into the force, into the Reserve and Guard Components, you know, the kind of skill sets and the people we need? Is that an issue for you?

To date the answer I have heard is, no, quite frankly, we have more people trying to get in than we really have space for in some ways. I have not heard the leadership come back to me and say no, this is really something that is a major issue. I am not trying to pretend it is not. I am just trying to highlight it hasn't when I have asked, bubble it to my level.

Each service has taken a slightly different approach for how it integrates Guard and Reserves into the broader structure. Some services are looking at Guard and Reserve as a cadre to augment the active side.

Other services, if you look at Army, for example, they are doing wholesale investments in building cyber capacity in the Guard and Reserve over and above what the cyber mission force needs. And Air Force is actually using Guard and Reserve as part of their cyber mission force build.

Mr. LAMBORN. Yes. That is what General Hyten was telling us——

Admiral ROGERS. Yes, sir.

Mr. LAMBORN [continuing]. Some of us at the space power caucus the other morning.

Thank you, Mr. Chairman. I yield back.

Mr. WILSON. And thank you very much, Congressman Lamborn.

We now proceed to Congressman Jim Cooper of Tennessee.

Mr. COOPER. I thank you, Mr. Chairman. Admiral, when a Congressman like Mr. Brooks asks you how we could get savings from the DOD budget, you might want to remind the members of the committee that we have banned the Pentagon from even thinking about any possible BRAC [Base Realignment and Closure] savings.

It would be illegal even though the Air Force I think has testified that 25 percent of their capacity is redundant surplus. So that is the easy savings that this committee has willfully ignored.

I am a little worried that I think on the Secretary's trip 2 weeks ago to Joint Base McChord, he met some very interesting people there and——

Admiral ROGERS. Right.

Mr. COOPER [continuing]. All the message he received was that it was easier to hire cyber experts before we bureaucratized everything. Now there is a requirement that you take a 6- to 9-month course and some of these folks we are trying to recruit could actually teach the course.

And they are not going to sit through something like that just to get their stripes when they already have all the skills that we are seeking. So I hope that as we seek out these folks we don't discourage them from coming.

Admiral ROGERS. Can I make a comment on that?

Mr. COOPER. Sure.

Admiral ROGERS. We have created a capability in the regular force that we call our equivalency board, because my concern was, look, we don't want to do a cookie cutter approach, one size fits all, in which we have a formalized process that we give equivalent

credit to people based on experience and not just, hey, did you go to military course X, Y, or Z?

So far I think we have approved almost 500 individuals where we have just granted credit for equivalent experience.

We are in the beginnings of an initial discussion with the Guard and the Reserve about couldn't we use the same thought process on the Guard and Reserve side so we give people equivalent credit, if you will, for real life experience so we can be faster and more efficient?

Mr. COOPER. I also hope the Guard and Reserve will get up to speed on the locational advantages. I was under the impression from a briefing yesterday that one of the top Guard efforts in cyber will be located in Arkansas. And I don't believe you mentioned that on the list of your visits.

Admiral ROGERS. I didn't, but I am aware of it.

Mr. COOPER. And I would think, and I have got nothing against Arkansas, but it would not be as target-rich an environment as some other parts of the country. But it is we have got to make sure we are doing the right thing here.

Another question is this. If you were in command and it turned out in retrospect that during the duration of your command it had been hacked, and yet you were in charge of that throughout your tenure, you are retired now, what consequence should there be?

Admiral ROGERS. I don't like speaking in theoreticals, sir. What I generally tell people is, look, we all should be held accountable for our actions. I am the first to acknowledge as a commander I have accountability for the missions. And I don't duck that for one minute. I would rather not get into hypotheticals.

Mr. COOPER. Well, unfortunately, it may not be a hypothetical. I am not speaking of your case, but in the case of other folks.

Admiral ROGERS. Well, who knows, sir? It could be at some point in the future——

Mr. COOPER. Well——

Admiral ROGERS [continuing]. Rogers isn't at the job anymore and I am the first to acknowledge that.

Mr. COOPER. Well, this is an increasing challenge because it is hard to know necessarily when you have been hacked or not and what the consequences of that——

Admiral ROGERS. Yes, sir.

Mr. COOPER [continuing]. Are. So it is a very ambiguous area. Is it currently against the Uniform Code of Military Justice to use improper computer hygiene? Like, it is my impression that you can be a commanding officer and lose your command if you commit adultery, but you can pollute the SIPRNET [Secure Internet Protocol Router Network] and it is really not a legal infraction.

Admiral ROGERS. I will say we are having an ongoing discussion about we have a very, as you have highlighted, we have got a very formalized and long practice mechanisms of accountability for performance in a lot of other areas.

How do we ensure that we do that same approach in cyber, because one of the concerns that I have, and I have mentioned this to the committee before, is you can have the greatest defensive structure in the world but the individual actions of every individual

user that we have can make our ability to actually take full advantage of those investments and those capabilities very difficult.

And you saw that in the Joint Staff intrusion, for example, where ultimately we were able to defeat the attempt in almost 60 other networks simultaneously except in this one particular network. The final defense is the user. In this case we had users who clicked on a link that I said what? What would lead you to do this? You know, read this. It doesn't make any sense.

And as a result of this, we are spending time, we are spending money. We have got mission operational impact here. We can't afford to have this sort of thing. It is one of the reasons why the previous vice chairman in particular felt very strongly we have got to create this culture of accountability.

So we have created an initiative. We call it DC3I [Defense Cybersecurity Culture and Compliance Initiative] and U.S. Cyber Command is the lead for the Department, about what are the kinds of steps we have to do to create that culture of accountability.

Mr. COOPER. Thank you. I see my time has expired.

Mr. WILSON. Thank you, Congressman Cooper.

And now I will proceed to Congresswoman Elise Stefanik, of New York.

Ms. STEFANIK. Thank you, Chairman Wilson and thank you Chairman for the great question on the Internet of Things where we are facing unique challenges as mobile devices and household devices become more interconnected. That increases the likelihood of cyber vulnerabilities. So it is a great question and I want to continue working with you on that issue.

Admiral Rogers, thank you for being here today, and thank you for your service to our country. Through the posture hearings from the past few months, we have heard about the evolving strategic threats in the cyber realm from a resurgent Russia, destabilizing threats from both state and non-state actors in the Middle East, and overt provocative cyber activity coming out of the Pacific region.

So today I want to focus my questions on the evolutions of these threats and how we maintain the edge on the 21st century battlefield. How confident are you moving forward that our cyber capabilities are robust enough to face the threats of the future on these multiple fronts? And then can you speak specifically to your concerns about adversarial cyber capabilities and your assessment of our own cyber capabilities moving forward?

Admiral ROGERS. So I feel comfortable with our level of capability. I have yet to run into a threat scenario that we didn't have the expertise to deal with. What concerns me is capacity, how much of it do you have?

And as the threats proliferate, our ability to deal with high-end simultaneous complicated threats. That is probably the biggest limiting factor for right now, which is why generating the mission force is so critical. That gives us that capacity as well as the tools and the other investments we are asking the committee and the Nation to support to get us to that capacity.

In terms of evolution of the threat as I look into the future I am going to riff off for just a little and if it doesn't get to your question, ma'am, you please just tell me.

As I look at the evolution of the threat what concerns me is you are seeing the last 18 months data in massive quantities now in and of itself has a value that previously we would have said to ourselves, look, this dataset is so large nobody can really do anything with it.

OPM, Anthem, those are good examples to us of data now is a commodity that has a value for a variety of purposes, whether that be counterintelligence, whether it be social engineering and helping to refine cyber activity, you will see increased attacks against big data concentrations is a trend of the future.

You are watching nation-states right now create relationships in many cases with a much broader range of actors out there than we traditionally had seen. I think this is in no small part an attempt to obscure what the real originator and director of the activity is.

It potentially or theoretically makes it more difficult for us to go to country X and say, hey, we see this activity going on. You are doing it. This is unacceptable to us.

And their ability to say, it is not us. It is a criminal group. It is some other actor. You have criminals in the United States, don't you? You don't control all that. We don't control all that.

So you are watching nation-states create these partnerships, I think in no small part to try to obscure our ability to highlight that their activity. Criminal activity continues to get more sophisticated. You are going to see a lot more ransomware. You watch over the next year you will see a lot more ransomware activity.

Ms. STEFANIK. So based on the fiscal year 2017 requested increase in funding for cyber capabilities, development, and operational support that you noted before, where do you feel the cyber community is assuming risk for readiness?

Admiral ROGERS. So we are still taking more risk than I would like. You look at individual platforms and weapons systems. Just because of the scale of the investments, because literally you are trying to overcome decades of investment in which redundancy, reliability, and defensibility against a cyber threat were just not core design characteristics.

And just as you highlighted in your comment about the Internet of Things, this increased connectivity and eternal connections that we developed in our system, not for bad reasons. I am not trying to criticize that for one minute.

If you are interested in designing—as a naval officer if you are in there interested in designing hull forms for future service combatants, you are interested in understanding how hull forms today are responding to different sea states around the world.

So you put telemetry and measurement devices and then now you are measuring it remotely. That also represents a potential threat vector now for someone to gain access.

So we are literally trying to overcome decades of investment in a very different threat world. So it is all about prioritization, and it is going to take us some measure of time to overcome or change that investment strategy.

So that would probably be the biggest area in some ways where you never have all you want. And particularly in this mission we are only 6 years old. In May, we will celebrate our sixth birthday, so, you know, we are new to this.

Ms. STEFANIK. Well, as you need those resources it is important for you to continue telling us on this committee to make sure that we are able to maintain the capabilities for our cyber capabilities moving forward. So thank you so much for the thoughtful answer.

Mr. WILSON. And thank you, Congresswoman Stefanik.

We now proceed to Congressman Joaquin Castro, of Texas.

Mr. CASTRO. Thank you, Chairman, and thank you, Admiral for——

Admiral ROGERS. Sir.

Mr. CASTRO [continuing]. Your testimony here today. I represent San Antonio, Texas, of course a very big military town, and my district includes Lackland Air Force Base, very proudly home of the 24th Air Force.

And so I want to ask a question about the cyber operators. Have you encountered any issues within the security clearance process in recruiting cyber operators?

Admiral ROGERS. I won't say there is none. Nothing that has led me to believe we have got a systematic problem that requires fundamental change. We always are looking to see can we accelerate or make this faster.

If you have been doing this long enough it is—I just had a discussion with a brand new hire about a month ago who expressed frustration to me. And I said I know. We are working our way through it. I would only tell you that we will make you happy, young man.

Boy, compared to where we were 3 years ago, 5 years ago we are in a much better place. So it is something we continue to look at, but there is no easy answer here because it is all about that balance.

Mr. CASTRO. Right.

Admiral ROGERS. You are concerned about threat. On the other hand you realize, look, you can't execute the mission without good people. And you can't get good people in to do the work unless you get them through your system.

Mr. CASTRO. Sure. And you mentioned, you know, the speed of processing. Do you see a merit in fast-tracking for certain critical positions?

Admiral ROGERS. There might be for some. There are a handful of—if you look across the cyber mission force there is probably I would argue a handful of skill sets where it is either very difficult for us to replicate it in a military environment, so we look to the civilian sector.

Or the skill, the level of knowledge and experience really narrows down the population that is qualified to do the job, so to speak. Those might be a couple things worth looking at.

Mr. CASTRO. Sure. And we would love to hear your suggestions, you know, at the appropriate time if you do come up with them.

Admiral ROGERS. Yes, sir.

Mr. CASTRO. So thank you. I yield back, Chairman.

Admiral ROGERS. And if I could, I am actually going to be in San Antonio with the 24th and the 25th Air Force——

Mr. CASTRO. All right.

Admiral ROGERS [continuing]. In about 10 days, so——

Mr. CASTRO. Well, welcome.

Admiral ROGERS. Sir.

Mr. WILSON. And thank you very much, Congressman Castro, and Admiral, thank you for being here today. We had a really good turnout from members of the subcommittee because what you are doing is so important for our country and what your colleagues are doing. And however we can be supportive and it is obviously, remarkably, incredibly bipartisan.

Admiral ROGERS. Sir. Thank you.

Mr. WILSON. We are now adjourned.

[Whereupon, at 2:59 p.m., the subcommittee was adjourned.]

A P P E N D I X

MARCH 16, 2016

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 16, 2016

Chairman Wilson Opening Statement
Hearing:
"Fiscal Year 2017 Budget Request for U.S. Cyber Command: Preparing for Operations in the Cyber Domain"

March 16th 2016, 2:00pm, 2212

I call this hearing of the Emerging Threats and Capabilities subcommittee of the House Armed Services Committee to order.

I am pleased to welcome everyone here today for this hearing on the Fiscal Year 2017 Budget Request for United States Cyber Command. Since we last met to talk about the work of U.S. CYBERCOM, the news has been filled with stories that remind us of the critical job facing the Department of Defense. From the intrusion on the Joint Staff networks to the compromise of personal information of millions of government personnel and their families, cyber is proving to be both a domain of warfare on its own, as well as a key enabler for all other domains of war.

In looking through this most recent budget request, we should be asking ourselves some important questions:

Do we have the resources, people, cyber tools, and training needed to be effective?

Do we have the necessary policies and authorities to conduct cyber operations? What areas require additional refinement?

Are we deterring potential adversaries, and contributing to our overall national security?

As we tackle these tough questions, I would like to take the opportunity to welcome back our witness here today, Admiral Michael Rogers, Commander of U.S. Cyber Command

One of the major tasks Admiral Rogers has to contend with is how to operate in an environment with our inter-agency, international, and industry partners. I am pleased to hear that in a major upcoming exercise, entitled Cyber Guard 16, personnel from the House Administration staff will be participating. I am especially looking forward to hearing the plans for that exercise, and how we might also apply its lessons in defending the House of Representative's networks.

I'd like to turn now to my friend and Ranking Member, Mr. Jim Langevin from Rhode Island, for any comments he'd like to make.

STATEMENT OF

ADMIRAL MICHAEL S. ROGERS

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

16 MARCH 2016

Thank you, Chairman Wilson, Ranking Member Langevin, and Members of the Committee. I am pleased to appear before you today to talk about the opportunities and challenges facing U.S. Cyber Command (USCYBERCOM). I am honored to represent the men and women of this strong team in their work to secure Department of Defense networks and defend the interests and security of our nation, in cyberspace. I know you would be as proud of them as I am if you could see their commitment and successes on a daily basis as I do. We at USCYBERCOM welcome this opportunity to tell you how we are shifting from a focus on building the Command to an emphasis on operationalizing, sustaining, and expanding its capabilities.

By way of context, USCYBERCOM is a sub-unified command of U.S. Strategic Command (USSTRATCOM). Though USSTRATCOM is headquartered in Nebraska, we are located nearby in Maryland, where we share a corner of Fort Meade with the National Security Agency (NSA), which I also direct. Our Congressionally appropriated budget for Fiscal Year 2016 amounts to $466 million (that's $259 million for our Headquarters and $207 million for Cyber Mission Forces support). We have 963 billets for full-time employees, both military and civilian, working in USCYBERCOM's headquarters, plus another 409 contract employees. Our military contingents represent every one of the Armed Services, both active and Reserve, and they include Coast Guardsmen as well. USCYBERCOM comprises a headquarters organization and seven components: the Cyber National Mission Force, the Joint Force Headquarters-DoD Information Networks, plus joint force headquarters and growing forces at Army Cyber Command/Second Army, Marine Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, and Air Forces Cyber/24th Air Force. Our seventh partner, though not a component, is

U.S. Coast Guard Cyber. USCYBERCOM manpower reflects a true total force effort encompassing a robust active component along with both Guard and Reserve forces being fully integrated at all echelons from the highest levels of our USCYBERCOM headquarters to our Cyber Mission Forces. Our service components are leading our integration efforts and building surge capacity, and they are doing an outstanding job. While USCYBERCOM resides with NSA, the two organizations are distinct entities with separate missions, authorities, and resource streams. Neither is an arm of the other, and both perform vital tasks on behalf of our nation.

Current Threats and Potential Threats

USCYBERCOM's mission goes well beyond defending DoD's networks and systems against cyber threats and cyber responses to those threats. Since I spoke to you last year USCYBERCOM has seen an intensification of cyberspace operations by a range of state and non-state actors. A year ago I mentioned North Korea's brazen cyber operations to impair and intimidate Sony Pictures Entertainment. We have seen no repetition of such destructive assaults against targets in the United States. On the other hand, we have seen a wide range of malicious cyber activities, aimed against American targets and victims elsewhere around the world, and thus we are by no means sanguine about the overall trends in cyberspace.

In a public forum it can be difficult to explain the nuance and depth of the threats that we at USCYBERCOM see on a daily basis. We must, however, because Congress, the federal government, industry, allies, and the general public should understand the ability and determination of malicious cyber actors. Literally every American who has connected to a network has been affected, directly or indirectly, by cyber crime. By this point millions of us have had personal information stolen, or seen our accounts or credit compromised. Even if we

have so far avoided such problems, however, we all pay higher prices for our computers and software, our Internet service, and the goods we buy as a result of cyber-enabled theft. That burden weighs on the entire economy, costing jobs and dampening growth. Just as all our citizens have benefitted from the increased productivity and speed that cyber commerce facilitates, all likewise pay the costs of cyber crime. This multi-faceted problem is the context for what follows.

At USCYBERCOM, as in the Department of Defense writ large, we focus on foreign state and non-state actors who would harm our national interests in cyberspace. Criminal activity remains the largest segment of cyber activity of concern, but nations in many ways still represent the gravest threats, as they alone can bring to bear the skills, the resources, and the patience to sustain sophisticated campaigns to penetrate and compromise some of the world's best-guarded networks. If they can gain access to those networks, moreover, they can manipulate information or software, destroy data, harm the computers that host those data, and even impair the functioning of systems that those computers control. We remain vigilant in preparing for future threats, as cyber attacks could cause catastrophic damage to portions of our power grid, communications networks, and vital services. Damaging attacks have already occurred in Europe. Just before Christmas, malicious actors launched coordinated cyber-attacks on Ukraine's power grid, causing outages and damaging electricity control systems. If directed at the critical infrastructure that supports our nation's military, cyber attacks could hamper our forces, interfering with deployments, command and control, and supply functions, in addition to the broader impact such events could have across our society.

The states that we watch most closely in cyberspace remain Russia, China, Iran, and North Korea. Russia has very capable cyber operators who can and do work with speed,

precision, and stealth. Russia is also home to a substantial segment of the world's most sophisticated cyber criminals, who have found victims all over the world. We believe there is some overlap between the state-sponsored and criminal elements in cyberspace, which is of concern because Russian actions have posed challenges to the international order.

China's leaders pledged in September 2015 to refrain from sponsoring cyber-enabled theft of trade secrets for commercial gain. Nonetheless, cyber operations from China are still targeting and exploiting U.S. government, defense industry, academic, and private computer networks. As Director of National Intelligence James Clapper testified last month, "China continues cyber espionage against the United States. Whether China's commitment of last September moderates its economic espionage remains to be seen."

Iran and North Korea represent lesser but still serious challenges to U.S. interests. Although both states have been more restrained in this last year in terms of cyber activity directed against us, they remain quite active and are steadily improving their capabilities, which often hide in the overall worldwide noise of cybercrime. Both of these nations have encouraged malicious cyber activity against the United States and their neighbors, but they currently devote the bulk of their resources and effort to working against their neighbors.

The so-called Islamic State in Iraq and the Levant (ISIL) is also a concern, though their organic capabilities to conduct malicious cyber activities so far remain limited and their main effort in cyberspace appears to be propaganda, recruiting, radicalization, and fundraising. ISIL has sought repeatedly to reach over our forces in the Middle East and carry the conflict into America itself. For instance, ISIL-affiliated cyber operators last spring posted the personal information of more than one hundred American service personnel, many of whom were here in the continental United States. Not only did the hackers for ISIL publicize the personal details on

these Americans, but ISIL also called for jihad against them, urging followers in the United States to assassinate them and their family members. While there is no direct link between this ISIL posting of personal information on service members and the recent extremist shootings in the U.S. and France, ISIL wants its followers on the Internet to take inspiration from such attacks.

In general all these various actors mount a range of cyber activities to support their interests in: a) fostering a nationalist vision of economic competition; b) intimidating émigré groups and neighbors whom they view as competitors; and c) deterring any perceived threats from other states, including ours. They steal from our corporations, and we learned last year that certain actors also stole the personal information of more than 21 million Americans that was stored in systems maintained by the Office of Personnel Management. Another group of hackers was responsible for an intrusion into an unclassified network maintained by our Joint Staff. Finally, we have seen cyber actors from more than one nation exploring the networks of our nation's critical infrastructure—and can potentially return at a time of their choosing. Collectively these actors make our government, our institutions, and our people spend far more on defense than the actors themselves spend on their efforts to penetrate our systems.

Some of these threat actors are seeking to shape us, narrowing our options in international affairs to limit our choices in the event of a crisis. As a result of these developments, we at USCYBERCOM are thinking more strategically about shifting our response planning from fighting a war to also providing decision makers with options to deter and forestall a conflict before it begins. These new options would be in addition to capabilities that help our combatant commanders succeed in their missions if and when conflict erupts and the joint forces receive an "execute order" to commence kinetic as well as cyberspace operations.

All of this work must be seen in the context of the Department's evolution of thinking toward what senior leaders call the "Third Offset" and its promise for deterring conventional as well as nuclear war. USCYBERCOM stands ready to help develop and deploy the new cyber capabilities entailed in the Third Offset, particularly hardened command and control networks and autonomous countermeasures to cyber attacks. Finally, our efforts are also proceeding in tandem with a heightened collaboration across the federal departments, agencies, and industry aimed at increasing the costs (to adversaries) of malicious cyber activities.

Progress and Prospects

Let me give you some details on how we are responding to the trends noted above. Over the last year we continued constructing USCYBERCOM while operating it at an ever-faster tempo. We have begun to transition from the "building the force" mode to a "readiness" mode. Our operations kept us busy defending the Department's networks and systems while supporting the missions of the combatant commands, especially U.S. Central Command (USCENTCOM), assisting other U.S. government entities (as authorized and upon the request of the relevant agency), and building capabilities to defend the nation against significant cyberspace attacks.

Progress in Building the Cyber Mission Force. To understand where we are today it is necessary to glance back at how far we have come. The Department of Defense concluded several years ago that defending the nation in cyberspace requires a military capability, operating according to traditional military principles of organization for sustained expertise and accountability at a scale that lets us perform multiple missions simultaneously. When we started to build that capability in early 2013, we had no cyber mission force, no ability to generate or train such an entity, and scant ability to respond at scale to defensive requirements or

requirements from combatant commanders. Now we have 123 teams of a target total of 133; those teams comprise 4,990 people and will build to 6,187 when we finish. In terms of progress, we have 27 teams that are fully operational capable today, and 68 that have attained initial operating capability.

The application of military capability at scale is what the Cyber Mission Force (CMF) gives us in USCYBERCOM and in the Department as a whole. Our Combat Mission Teams (CMTs) operate with the combatant commands to support their missions, while National Mission Teams (NMTs) help defend the nation's critical infrastructure from malicious cyber activity of significant consequence. We have Cyber Protection Teams (CPTs) to defend DoD Information Networks alongside local Computer Network Defense Service Providers (CNDSPs). Each of them complements the efforts of the others. I should emphasize that Cyber Mission Force teams can and do contribute to our nation's cyberspace efforts even before they reach full operational capability. Elements of teams that are still "under construction" are already assisting the combatant commands and our partner departments and agencies. Cyber Protection Teams, for instance, played important roles in defending the Joint Staff's unclassified systems after an intrusion last summer, and in remediating the vulnerabilities that the intruders had utilized.

Those Cyber Mission Force teams give USCYBERCOM the capacity to operate on a full-time, global basis on behalf of the combatant commands. The Combat Mission Teams help combatant commanders accomplish their respective missions to guard U.S. interests and project our nation's power when authorized to deter those who would threaten our security—the teams help ensure that we have the ability to enable our combatant commanders to defeat emerging threats. Such assistance occurs daily, for instance, in the fight against ISIL, as Secretary Carter recently explained in his remarks in California. Although I cannot address the particulars in this

setting, USCYBERCOM is executing orders to make it more difficult for ISIL to plan or conduct attacks against the U.S. or our allies from their bases in Iraq and Syria to keep our Service men and women safer as they conduct kinetic operations to degrade, dismantle, and ultimately destroy ISIL. The nation and every combatant commander can now call on CMF teams to bring cyberspace effects in support of their operations. Additional Combat Mission Teams under the functional commands (U.S. Strategic Command, U.S. Transportation Command, and U.S. Special Operations Command) bring still more resources to supplement those of the regional commands.

At USCYBERCOM, moreover, we control additional teams under the Cyber National Mission Force (CNMF) that can help defend America's critical infrastructure against malicious cyber activity of significant consequence. The CNMF comprise National Mission Teams, National Support Teams, and National Cyber Protection Teams to conduct full-spectrum cyberspace operations to deter, disrupt, and defeat adversary cyber actors.

DODIN Operations and Defense: At USCYBERCOM we have extended the same principles (unity of effort and command for sustained effort at scale) to the operation and defense of DoD information systems. Last year I noted that we had just established the Joint Force Headquarters (JFHQ-DoDIN) and dual-hatted the Director of the Defense Information Systems Agency to command it. Today I can proudly report that JFHQ-DoDIN has made great strides toward its goal of leading the day-to-day defense of the Department's data and networks. As a functional component command of USCYBERCOM located at DISA, JFHQ-DoDIN directs an aggressive and agile network defense. The Department of Defense as a whole is working to harden and defend its networks and systems, with USCYBERCOM providing the operational vision and directing the defense, and the DoD Chief Information Officer (CIO), working with

NSA, DISA and the military services, providing the technical standards and implementation policy. DoD CIO is measuring the cyber security status of the whole department, and for particular missions through the new CIO cybersecurity scorecard, which is provided to the Secretary each month. The Secretary recently announced another initiative as well, linked to broader Administration efforts to strengthen the nation's cybersecurity under the Cyber National Action Plan—a "bug bounty" to encourage private-sector experts (i.e., trusted hackers) to probe our systems for vulnerabilities. The goal of all of these measures is to minimize the adversary's ability to attack our systems and networks, and to detect, diagnose, contain, and eject an adversary should an attack occur.

Our operations to defend DoD networks and the nation's critical infrastructure proceed in conjunction with a host of federal, industry, and international partners (about whom I shall say more in a moment). Defending America in cyberspace is a whole-of-government, indeed a whole-of-nation, endeavor. No single agency or department has the authority, information, or wisdom to accomplish this mission alone, which is why USCYBERCOM and NSA recently updated our understandings with the Department of Homeland Security in a cyber action plan to chart our collaboration. The entire federal government, however, cannot do the job without the active participation and cooperation of the private sector. Here I compliment Congress for recently passing the Cybersecurity Information Sharing Act, which should enable industry to increase its sharing of threat information with the federal government (and vice versa) without fear of losing competitive advantage or risking additional legal liability. This is a key element in the government's efforts to improve the cybersecurity of critical infrastructure—and to frustrate adversary attempts to bend American foreign policy to their liking or even to harm Americans.

We seek to build the Command's capabilities (especially the Cyber Mission Force) with deliberate speed, and progress continues to accelerate as we learn and improve at building our teams. We remain committed to achieving full operational capability for the entire CMF by the end of FY18. Our ability to do this is shaped in no small part by consistent funding throughout the remainder of the CMF build. The key to the CMF's utility to the Department and the nation is the proficiency of its personnel. We do our best to give our people the infrastructure, tools, and support they require, but military cyber operations, despite their high degree of automation, place a premium on insight, intuition, and judgment.

Training. Cyber operators are being trained to operate mission effectiveness (for the Department and for the nation), and they must operate in a manner that respects and protects the civil liberties and privacy of American citizens. Developing a training program for cyber operators resembles the challenge that DoD faces in training pilots and aircrew to operate some of the world's most advanced aircraft, maintaining their skills on the latest aircraft systems, and sustaining their numbers to ensure a constant sufficiency of motivated and technically excellent personnel. Creating such a "pipeline" in the U.S. military's (and other countries') air components took many years, so I am hardly surprised by the persistence and complexity of the challenges that we at USCYBERCOM confront in constructing the training and personnel pipeline for the Cyber Mission Force.

Sustainment. Training the force does not automatically bring it to peak proficiency. Teams must learn to operate against live opposition, and our commanders and seniors must develop an understanding of how cyber operations unfold so they have a better idea of what to expect and what can be achieved. USCYBERCOM has been providing some insights by employing teams in the recent series of real-world operations, such as in dealing with intrusions

in DoD systems and the networks of other federal entities. Cyber Mission Teams are now regular participants in the annual exercises of the geographic and functional combatant commands, even though the demand for CMF participation outstrips our capacity to provide teams to all the exercise organizers who request them. USCYBERCOM's own annual exercises, CYBER FLAG and CYBER GUARD, offer a certain degree of realism, assembling federal, state, industry, and international partners to practice cyber defense and offense against a wily opposition force. The realism they offer is limited, however, in part because they operate on simulated networks that do not come close to approximating the scale and complexity of the Internet. We can do better, which is why the Department is building for us an advanced Persistent Training Environment to exercise our teams, and though it is not yet complete it has already been used and found very helpful.

Capabilities. Our teams require specialized tools, infrastructures, and capabilities to perform their missions. The work of improving our ability to operate in cyberspace begins in our own DoD systems; our networks are continually being probed and frequently attacked, so we are learning to combine the insights we gain from these events with our knowledge of cybersecurity to achieve situational awareness and an intuitive feel for what is coming next. In addition, USCYBERCOM has partners that possess very useful capabilities and skills, so we are constantly seeking to expand our knowledge of what is under development in the Services, national labs, agencies, as well as key foreign partners.

Innovation. Secretary Carter spoke in California recently about the importance of innovation for DoD. We heartily agree, which is why our outreach to academia and to industry is expanding as well. In the last year we established a lean but motivated "Point of Partnership" in Silicon Valley to link Command personnel to some of the most innovative minds on earth.

This new unit will help industry understand how to interact with USCYBERCOM—both how we work and where to plug in so we can work difficult, and mutual, problems together. It will also help USCYBERCOM scout technology trends, build trust, and develop mechanisms and pilot projects to facilitate the movement of the nation's cyber workforce across the public-private boundary. Our Point of Partnership is aligned and co-located with the Department's new Defense Innovation Unit-Experimental (DIUx), and we are hoping for synergy among all the DoD elements under the DIUx umbrella. Another of our efforts in this area is an ongoing set of initiatives and projects to bolster the security of hardware and software in DoD weapons systems. We are learning a great deal from this effort.

Culture. Innovation, technical upgrades, and cyber organizational changes are ongoing and necessary but by themselves are insufficient to help us fully defend our networks, systems, and information. Last September, the Department identified the need to transform DoD cybersecurity culture by improving individual performance and accountability as called for in the DoD Cyber Strategy. The Secretary and Chairman approved the DoD Cybersecurity Culture and Compliance Initiative (DC3I) to initiate a shift in the Department's cybersecurity norms. This initiative seeks to instill principles of operational excellence, personal responsibility, and individual accountability into all who provide or use cyber capability to accomplish a mission. The Department already inculcates a culture of responsibility and accountability in every DoD affiliate, both uniformed and civilian, who is authorized to handle a firearm. Our reliance on networks and data systems to accomplish our missions demands all DoD personnel understand their individual responsibilities to protect the Department of Defense Information Networks and act with similar discipline and diligence everytime they use Department systems. Instituting meaningful and lasting cultural change DoD-wide will require a long-term commitment by the

Department. USCYBERCOM was identified as the mission lead for this initiative and is working closely with Joint Staff and the Office of the Secretary of Defense to build the capacity and structure to increase cybersecurity and promote mission assurance through improved human performance in cyberspace.

DoD Cyber Strategy. Another USCYBERCOM function is to help the Department's leadership to reflect and act on the full range of issues pertaining to the cyber field Many such issues fall outside our Command's mission set, strictly speaking, but still have relevance to how the United States can and should regard cybersecurity for the nation and cyberspace capabilities as an instrument of national power. We are called upon for contributions on matters such as the implementation of the new DoD Cyber Strategy, or the defense of personally identifying information of DoD personnel and affiliates in sensitive databases, because of our level of expertise on cyber matters. Senior leaders at the Command are leading teams or serving on all of the teams charged with implementing the DoD Cyber Strategy's many initiatives, particularly the "lines of effort" regarding the training and proficiency of cyber personnel as well as the integration of cyber effects in DoD and cross-agency planning efforts. We at USCYBERCOM, of course, consult constantly our network of partners across the U.S. government to learn more. Typically a combatant command, let alone a sub-unified command, is not staffed to play such a role for the Department, but cyberspace is a dynamic environment with a host of complicated and consequential issues, and DoD has not yet had time to build up the broad and deep reserve of institutional knowledge that it possesses on other matters.

Authorities. I thank Congress and the President again for the acquisition authorities granted to USCYBERCOM in the National Defense Authorization Act for Fiscal Year 2016. Together with new manpower flexibility these presage a significant augmentation of our role of

bringing capabilities to our cyber mission teams and network defenders, as well as our ability to keep our DoD cyber workforce proficient. We are studying how best to implement that Act's provisions—such as the role of a new Command Acquisition Executive and the scope of cyber operations-peculiar equipment and capabilities—and laying the groundwork needed to put its provisions into effect after the Department drafts its implementation plan.

DoD has extensive sharing arrangements already with some of our closest allies and partners, who support our operational planning and capabilities development. These arrangements are not unlimited, but they have improved our situational awareness and helped us in the maturation of USCYBERCOM, and we have a process for managing the relationships and extending collaboration in new areas as needed. Other nations engaged in the fight against violent extremists and in planning for contingencies involving potential adversaries have also expressed their desire to partner with us. We are more limited in what we can do with them.

Let me head toward a conclusion by reflecting on how we can take advantage of the new authorities and changes discussed above in building a cyber force that is even more capable in the future. As we learn how to conduct operations to defend our nation in cyberspace, our experiences are convincing me that we across the Department may need to think again about what a 21st century military organization is. When we created USCYBERCOM we did so with the understanding that our basic principles and values remain sound; our Command was constructed to apply time-honored lessons about the need for clear and unified authorities, for consistent performance at scale, for sustainability, and for a capacity to synchronize a wide range of activities under the rule of law. I marvel at this nation's ability to assemble such resources and operate them in such a powerful manner, and I also marvel at the commitment and skill of our people—active duty and civilians alike—who answered the call to service in this new

domain. Terrorists can harm us but they have no chance of defeating such a force as long as we remain true to our national values. Nevertheless, terrorism is not the only threat we face. Other states will one day build cyber forces as capable as ours and they may attain comparable capabilities, just as the Soviets achieved rough nuclear parity with us in the Cold War. Military power in cyberspace is already something of a misnomer; cyber forces do not square off against each other and fight pitched battles like armies or fleets. Indeed, cyberspace is unlike the natural domains in many ways, and thus certain metaphors and analogies from the natural domains might just confuse matters and impair judgment. Our new cyber military force is virtually always a partner, as it rarely, if ever, acts alone. Instead, it can constitute the center of gravity for joint and combined, whole-of-government operations that defend the United States and serve the interests of the nation, and its people, and our allies. The President's *International Strategy for Cyberspace* clearly articulates our policy to exhaust other options short of military force if possible, but it also emphasizes our nation's inherent right of self-defense in cyberspace and all other domains. To exercise that right, our nation must understand how others might use force against us, and to do so we must know how force works in cyberspace, and why our nation must be able at times to depend on military capabilities that act as a nucleus of national power in this domain.

Conclusion

Thank you again, Mr. Chairman, Ranking Member Langevin, and Members of the Committee, for inviting me to speak to you today. I greatly appreciate the support that you and this Committee have provided to USCYBERCOM, and I am also grateful for the stability that you and your colleagues in Congress have provided to our resource base over the next couple

years as we complete the Cyber Mission Force build and shift our focus to sustained operations. We look to your counsel as we partner with the federal government, industry, allies, and the whole gamut of stakeholders who seek to preserve cyberspace as a free, reliable, and secure domain for exchange, commerce, culture, and progress. Our nation determined some years back that preserving freedom and security in cyberspace will inevitably mean an operational role for the U.S. military in this domain. We at USCYBERCOM strive every day to provide the sort of military capabilities and options that our leadership requires to secure and defend DoD information systems and to protect and further the nation's interests, not only in cyberspace but in all domains where our national security is challenged. I hope you will agree that our people at USCYBERCOM—while their work is not done—have already delivered handsomely on the early promise that you saw and supported. They take pride in their accomplishments, but they do not rest on them. With them, I look forward to tackling our current and future challenges together with you and our mission partners across the government. I am happy to take your questions.

Admiral Michael S. Rogers
Commander, U.S. Cyber Command
Director, National Security Agency
Chief, Central Security Service

Admiral Michael Rogers is a native of Chicago and attended Auburn University, graduating in 1981 and receiving his commission via the Naval Reserve Officers Training Corps. Originally a surface warfare officer (SWO), he was selected for re-designation to cryptology (now Information Warfare) in 1986.

He assumed his present duties as commander, U.S. Cyber Command and director, National Security Agency/Chief, Central Security Service in March 2014.

Since becoming a flag officer in 2007, Rogers has also served as the director for Intelligence for both the Joint Chiefs of Staff and U.S. Pacific Command, and most recently as commander, U.S. Fleet Cyber Command/U.S. 10th Fleet.

Duties afloat have included service at the unit level as a SWO aboard USS Caron (DD 970); at the strike group level as the senior cryptologist on the staff of commander, Carrier Group 2/John F. Kennedy Carrier Strike Group; and at the numbered fleet level on the staff of Commander, U.S. 6th Fleet embarked in USS Lasalle (AGF 3) as the fleet information operations (IO) officer and fleet cryptologist. He has also led cryptologic direct support missions aboard U.S. submarines and surface units in the Arabian Gulf and Mediterranean.

Ashore, Rogers commanded Naval Security Group Activity Winter Harbor, Maine (1998-2000); and, has served at Naval Security Group Department; NAVCOMSTA Rota, Spain; Naval Military Personnel Command; Commander in Chief, U.S. Atlantic Fleet; the Bureau of Personnel as the cryptologic junior officer detailer; and, Commander, Naval Security Group Command as aide and executive assistant (EA) to the commander.

Rogers' joint service both afloat and ashore has been extensive and, prior to becoming a flag officer, he served at U.S. Atlantic Command, CJTF 120 Operation Support Democracy (Haiti), Joint Force Maritime Component Commander, Europe, and the Joint Staff. His Joint Staff duties (2003-2007) included leadership of the J3 Computer Network Attack/Defense and IO Operations shops, EA to the J3, EA to two directors of the Joint Staff, special assistant to the Chairman of the Joint Chiefs of Staff, director of the Chairman's Action Group, and a leader of the JCS Joint Strategic Working Group.

Rogers is a distinguished graduate of the National War College and a graduate of highest distinction from the Naval War College. He is also a Massachusetts Institute of Technology Seminar XXI fellow; Harvard Senior Executive in National Security alum; and holds a Master of Science in National Security Strategy.

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MARCH 16, 2016

QUESTIONS SUBMITTED BY MR. WILSON

Mr. WILSON. What are the most common and consequential types of cyber incidents that affect public safety or critical infrastructure security in the United States? Do the Department of Defense and National Guard assist with response to domestic cyber incidents that threaten public safety or critical infrastructure security, or do you expect that they will need to do so in the future? If so, how are they preparing for these incidents?

Admiral ROGERS. Consequential cyber incidents affecting the public safety or critical infrastructure security in the United States include attacks which degrade or disrupt major functions of the 16 critical infrastructure sectors identified in Presidential Policy Directive 21 (PPD–21), Critical Infrastructure Security Resilience. According to PPD–21, each sector "... provides the essential services that underpin American society." Disruption of any of these services for a significant period of time would have an impact on public safety. Potential cyber incidents include attacks which achieve unauthorized access, destroy data or system function, or result in release of sensitive information.

The Department of Homeland Security (DHS) is the lead for domestic incident response to cyber incidents. If unable to address a cyber incident, the DHS may submit a Defense Support to Civil Authority (DSCA) request which potentially could task resources through the DOD, USSTRATCOM, and ultimately USCYBERCOM. Currently this scenario is viewed as a last resort situation.

The National Guard assigned cyber forces are available to support any federal response in Title 10 status or State response in either State Active Duty (SAD) or when authorized in Title 32 status. Ensuring the National Guard cyber forces are properly manned, trained, and equipped for any particular mission set, is key. The DOD, National Guard, and DHS have trained to respond to cyber incidences, as part of a Whole-of-Nation approach, through exercises like CYBER GUARD.

Mr. WILSON. To what extent has U.S. Cyber Command collected measures of performance or measures of effectiveness to demonstrate that the dual-hatted position with the National Security Agency is the most effective and most efficient approach to both agencies missions?

Admiral ROGERS. USCYBERCOM has focused its assessment efforts on evaluating its growing resource requirements, increasing support to the Geographic Combatant Commanders' plans, named cyber operations, and the Department's requirements for information network security. Our assessment program reviews and analyzes progress towards achieving campaign plans objectives but has not studied alternative command structures. To date, we have not collected measures of performance or effectiveness to demonstrate that the dual-hat approach is the most effective and efficient approach. USCYBERCOM is reliant on the National Security Agency to accomplish large portions of our missions, which requires close and continual technical coordination.

QUESTIONS SUBMITTED BY MR. LAMBORN

Mr. LAMBORN. Given the rapidly growing demand for CMF training, do you think DOD needs to begin to look at other ways to deliver training, including through greater influencing courses offered at university, and by developing commercial training opportunities?

Admiral ROGERS. DOD continues to examine the most effective means to deliver joint training for the Cyber Mission Force (CMF). CMF training provided by the Services and the National Security Agency (NSA) Cryptologic Training System (CTS) rely on both government and contractor provided training courses. Currently 60% of the NSA offered courses that are on the CMF Training Pipeline are instructed by commercial vendors. We are working with NSA to continue to leverage their robust academic outreach programs to connect with government (e.g., National Defense University, Defense Cyberspace Investigation Training Academy, service academies, war colleges) and universities/colleges.

Mr. LAMBORN. What standards do CPT personnel have to meet in order for them to be fully qualified cyber defenders? Please provide a copy of the standards to the Committee.

Admiral ROGERS. In accordance with the Cyber Mission Force (CMF) Training Model, Cyber Protection Team (CPT) personnel must meet the standards for individual proficiency contained in the USCYBERCOM Joint Cyberspace Training and Certification Standards (JCT&CS) and team/force proficiency in the Training and Readiness (T&R) Manual in order for them to be fully qualified cyber defenders. The JCT&CS provide the specific knowledge, skill and ability standards for each CMF work role at the apprentice, intermediate and expert levels. The T&R Manual provides the development, execution, and assessment of collective (squad, team, headquarters) training to support force development and readiness.

The CMF Training Model is a phased training process based on mission-specific requirements and tasks. Personnel assigned to a CPT begin with a mix of foundation training or Service equivalent training, then move to specialized technical/tradecraft instruction, and localized individual technical joint qualification record (JQR) and on the job training (OJT), coupled with an intensive staff and collective training and exercise program to achieve mission readiness. Collective training activities are an extension of individual proficiency to team and unit proficiency. An example of a collective training event for CPT Teams is the CYBER GUARD exercise, which is focused on exercising a whole of nation defense of U.S. critical infrastructure from destructive cyber attack.

When a CPT member has met their JCT&CS work role specific individual tasks, JQR/OJT, and participated in team collective training event assessed using the T&R manual, they are then considered a fully qualified cyber defender.

Mr. LAMBORN. Who is responsible for training CPTs, and do you believe the CPTs have enough training to effectively protect our networks against advanced cyber adversaries like Russia and China? How do you plan to get the CPTs capable of defending against such threats? Are the Services doing their part to train the CPTs?

Admiral ROGERS. The military Services and U.S. Cyber Command, working with the National Security Agency (NSA), are responsible for training CPTs. No, we do not yet believe CPTs have enough training to effectively protect our networks against advanced cyber adversaries. However, we are making significant progress in maturing and expanding training to achieve required levels of operational readiness for CPTs.

We have a strong program in place for Cyber Mission Force (CMF) individual training and qualification to joint standards for personnel assigned to CPTs. Personnel begin with Service-provided training in a primary specialty, and then once assigned to a CPT each person completes work role-specific training and qualification to rigorous joint standards under a system managed by U.S. Cyber Command, working with the National Security Agency's Cryptologic Training System. This individual training process provides the baseline for individual proficiency. We continue to mature the individual training process as we grow the CMF and the Services are fully involved in that process and doing their part. The Services are expanding Service-provided training to deliver outcomes that meet joint standards for the CPTs.

We do not yet have sufficient collective training capacity for CPTs because we still lack a Persistent Training Environment (PTE) for DOD cyberspace forces. CPTs are not groups of trained technicians, but maneuver forces that must operate as a disciplined fighting force to perform assigned missions against determined adversaries. That requires CPTs conduct collective training in a closed network environment in realistic operational scenarios against an opposing force simulating advanced cyber adversaries. That enables our forces to train as they fight. We currently use limited, existing DOD capabilities to conduct periodic collective training and exercises, such as CYBER FLAG and CYBER GUARD. However, we don't have sufficient training capability or capacity to train continuously to achieve or sustain the levels of required readiness for all CPTs. The PTE for cyberspace forces that is included in the President's FY17 Budget Request is essential to providing the capability needed to train CPTs, along with the entire Department of Defense cyberspace workforce. The PTE will enable us to train CPTs to effectively protect our networks against advanced adversaries.

Beyond training, we are preparing CPTs to address threats by leveraging expertise from across the government, including NSA and the Services' network defenders that have experience in this area. We are building capability to better posture our teams against high level malicious cyber actors through the utilization of incident response teams, increased use of intelligence to understand the threat, identification of unique network technology in specialized systems (Industrial Control Systems/Supervisory Control and Data Acquisition, etc.), and by building a more detailed un-

derstanding of critical infrastructure and key resource vulnerabilities. Finally, we are strengthening partnerships within government, with allies and the private sector to train and operate together. We believe that these initiatives, along with training, will ensure the CPTs achieve and sustain readiness to defend against such threats.

Mr. LAMBORN. On a yearly basis, how many hours of live, on-network training with a realistic cyber-adversary do CPT personnel receive in order to ensure they can hone their defensive cyber skills? Do you think this training is sufficient, and if not, how do you plan to increase the amount of realistic training the CPT personnel receive?

Admiral ROGERS. At this time, it is difficult to quantify the exact number of live, on-network hours our Cyber Protection Team (CPT) personnel receive on an annual basis as we continue to mature CPT training/methodologies and work through certifying teams currently in the build phase. USCYBERCOM hosts two major cyber exercises (CYBER GUARD and CYBER FLAG) and numerous team-level exercises (CYBER KNIGHT) each year, which offer a certain degree of realism against an advanced cyber-adversary. In CYBER GUARD and CYBER FLAG, a CPT receives a minimum of 60 hours in each exercise of live, on-network training against a realistic cyber-adversary. Combatant Command Tier 1 level exercises provide additional opportunities for training the Cyber Mission Force (CMF) via red teams emulating advanced adversary tactics, techniques, and procedures (TTPs). The intelligence community works in coordination with the red teams to ensure realistic cyber adversary TTPs are utilized and that defenders are exposed to current and future cyber adversary TTPs to ensure quality training is continuously achieved. The realism these exercises offers is limited, in part because the teams operate on simulated networks that do not come close to approximating the scale and complexity of the Internet.

USCYBERCOM recognizes there is currently a capacity issue in terms of realistic training opportunities for our CPT personnel, which is why a Persistent Training Environment (PTE) and all of its elements are critical to the training and readiness of the CMF. The PTE, a geographically distributed, federated system of interconnected capabilities (not just a coalition of cyber training ranges), provides an integrated common training capability to deliver individual and collective training outcomes for DOD cyberspace forces to generate and sustain force readiness across the full spectrum of operations from the tactical to strategic level of conflict. The DOD cyber forces require a Joint PTE with sufficient capacity to ensure geographically dispersed teams across the total force are fully prepared to conduct current cyberspace operations and future scenarios involving cyberspace operations consistent with approved plans (e.g., CONPLANs, OPLANs, etc.).

Mr. LAMBORN. As the Department moves toward JIE and a government-owned, contractor-operated model for its core infrastructure, what is the plan for the thousands of civil service IT professionals currently maintaining this infrastructure? Will they be retrained for assignment to a CPT or CMF, and do current legal authorities allow for civilian participation in these Title 10 activities?

Admiral ROGERS. A tenant of JIE is to align DOD Component IT capabilities by bringing them together under an enterprise services construct to leverage economies of scale in terms of IT resources, money and manpower. Traditionally, DOD Components are responsible for deploying capabilities, as well as manning, training and equipping their IT workforces to meet mission requirements. Workforce efficiencies gained as a result of JIE would be available for DOD Components to repurpose. There may be a need for retraining of duties, re-scoping of responsibilities or leveraging existing skills with no additional training required.

The Department is in the process of developing and implementing initiatives which could assist the DOD components to identify options for reassigning personnel. The DOD Cyberspace Workforce Framework (DCWF) provides descriptions for 54 cyber work roles and was developed from the National Initiative for Cybersecurity Education, Cybersecurity Workforce Framework, and the USCYBERCOM Joint Cyberspace Training Certification Standards (JCT&CS). Additionally, the DCWF contains a cross-functional analysis that identifies the knowledge, skill and ability deviations between each role. Furthermore, CMF training will be more widely available as the Services continue to advance on the training transition plan. The availability of additional training such as CMF training will assist with personnel transitioning from traditional IT and network operations roles into cybersecurity or cyberspace effects roles. The CMF would benefit from a workforce trained in network engineering, incident response, and other cyber disciplines. IT professionals' careers may be re-scoped to support tasks within the Defend the Nation (DTN), Offensive Cyberspace Operations (OCO) and Defensive Cyberspace Operations (DCO) missions. DOD civil servants currently serve across the CMF and can, consistent with law and policy, participate in the CMF's Title 10 activities.

Additionally, DOD Components may leverage their civil service IT professionals to support emerging IT initiatives, including protection of Industrial Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA) and enabling mobility capabilities. Portions of a DOD Components' workforce can be retrained to perform Defensive Cyberspace Operations—Internal Defensive Measures (DCO–IDM) actions such as Cybersecurity Service Provider duties.

Some examples of USCYBERCOM's vision for possible manpower realignment:

—Retrain and Repurpose within the Combatant Commands, Services and Agencies: Support to emerging IT initiatives, including protection of Industrial Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA) and enabling mobility capabilities may require a degree of retraining. Portions of a Component's workforce can be retrained to perform defensive cyberspace actions such as Cybersecurity Service Provider duties and augmenting cybersecurity capability readiness.

—Retrain and Repurpose of the Cyber Mission Force (CMF): The CMF could benefit from a workforce trained in network engineering, incident response, and other cyber disciplines. Careers may be re-scoped to support tasks within the Defend the Nation (DTN), Offensive Cyberspace Operations (OCO) and Defensive Cyberspace Operations (DCO) missions.

—Migrate to an IT-focused Combat Support Agency (CSA): The Defense Information Systems Agency (DISA) and the National Security Agency (NSA) have large roles in architecting, engineering and maintaining JIE Enterprise Services. Portions of the workforce formerly operating IT capabilities on behalf of a DOD Component could be leveraged by CSAs to continue supporting the global DOD Cyber Operations Mission.

—Reduction in Force: Personnel who decline to undertake one of the above options could be reassigned into other mission areas, or reduced through attrition. It is at the discretion of the individual DOD Component to determine how to best undertake this option.

The move toward JIE provides an opportunity for the existing IT workforce to retrain, re-scope and realign high-demand low-density positions with emerging mission requirements.

○